04-03-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

**Attorney Docket No.** 042390.P7948 Total Pages 2

**First Named Inventor or Application Identifier** Robert W. Faber

**Express Mail Label No.** EL431686001US

**ADDRESS TO:** **Assistant Commissioner for Patents**
**Box Patent Application**
**Washington, D. C. 20231**

**APPLICATION ELEMENTS**
See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 33 )
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 4 )

4. X Oath or Declaration (Total Pages 7 )

a. X Newly Executed (Original or Copy)

b. ___ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**

i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. _ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. _ Microfiche Computer Program (Appendix)

7. ____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

8. ____ Assignment Papers (cover sheet & documents(s))

9. ____ a. 37 CFR 3.73(b) Statement (where there is an assignee)

_X_ b. Power of Attorney

10. ____ English Translation Document (if applicable)

11. ____ a. Information Disclosure Statement (IDS)/PTO-1449

____ b. Copies of IDS Citations

12. ____ Preliminary Amendment

13. _X_ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

14. ____ a. Small Entity Statement(s)

b. Statement filed in prior application, Status still proper and desired

15. ____ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. _X_ Other: separate sheet with title, express mail label, copy of postcard and attorney's signature

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

____ Continuation ____ Divisional _X_ Continuation-in-part (CIP)

of prior application No: 09/385,590, 09/385,592

18. **Correspondence Address**

____ Customer Number or Bar Code Label ____________
(Insert Customer No. or Attach Bar Code Label here)

or

**_X_** Correspondence Address Below

NAME Aloysius T.C. AuYeung
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard
Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (425) 827-8600 FAX (425) 827-5644

Express Mail Label: EL431686001US

Our Reference: 042390.P7948 *Patent*

METHOD AND APPARATUS FOR PROTECTED EXCHANGE OF STATUS AND SECRET VALUES BETWEEN A VIDEO SOURCE APPLICATION AND A VIDEO HARDWARE INTERFACE

Inventors: Robert W. Faber, David A. Lee, Brendan S. Traw, Gary L. Graunke, and Richard P. Mangold

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Aloysius T.C. AuYeung
Reg. No. 35,432

"Express Mail" mailing label number: EL431686001US
Date of Deposit: March 31, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231

**Dominique Valentino**
(Typed or printed name of person mailing paper or fee)
Dominique Valentino 3-31-00
(Signature of person mailing paper or fee) (Date signed)

Serial/Patent No.: Not Yet Assigned Filing/Issue Date: Herewith
Client: Intel Corporation
Title: METHOD AND APPARATUS FOR PROTECTED EXCHANGE OF STATUS AND SECRET VALUES BETWEEN A VIDEO SOURCE APPLICATION AND A VIDEO HARDWARE INTERFACE
BSTZ File No.: 042390.P7948 Atty/Secty Initials: ATA/dcv
Date Mailed: March 31, 2000 Docket Due Date:

**The following has been received in the U.S. Patent & Trademark Office on the date stamped hereon:**

□ Amendment/Response (_____ pgs.)
□ Appeal Brief (_____ pgs.) (in triplicate)
□ Application - Utility (_____ pgs., with cover and abstract)
□ Application - Rule 1.53(b) Continuation (_____ pgs.)
□ Application - Rule 1.53(b) Divisional (_____ pgs.)
■ Application - Rule 1.53(b) CIP (33 pgs.)
□ Application - Rule 1.53(d) CPA Transmittal (_____ pgs.)
□ Application - Design (_____ pgs.)
□ Application - PCT (_____ pgs.)
□ Application - Provisional (_____ pgs.)
□ Assignment and Cover Sheet
■ Certificate of Mailing
■ Declaration & POA (7 pgs.) (unsigned)
□ Disclosure Docs & Orig & Copy of Inventor's Signed Letter (_____ pgs)
□ Drawings: 4 # of sheets includes 8 figures

■ Express Mail No.: EL431686001US
□ ________ Month(s) Extension of Time
□ Information Disclosure Statement & PTO-1449 (__ pgs.)
□ Issue Fee Transmittal
□ Notice of Appeal
□ Petition for Extension of Time
□ Petition for __________
■ Postcard
□ Power of Attorney (_____ pgs.)
□ Preliminary Amendment (_____ pgs.)
□ Reply Brief (_____ pgs.)
□ Response to Notice of Missing Parts
□ Small Entity Declaration for Indep. Inventor/Small Business
■ Transmittal Letter, in duplicate
■ Fee Transmittal, in duplicate

■ Check No. 000372
Amt: $1,602.00
□ Check No. ______
Amt: ______

■ Other: Certificate of mailing with copy of return postcard signed by attorney

Our Ref.: 42390.P7948

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

# Method And Apparatus For Protected Exchange Of Status And Secret Values Between A Video Source Application And A Video Hardware Interface

Inventor(s): **Robert W. Faber**
**David A. Lee**
**Brendan S. Traw**
**Gary L. Graunke**
**Richard P. Mangold**

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard, 7th Floor
Los Angeles, California 90025
(503) 684-6200

*"Express Mail" Label Number* *EL431686001US*

# Method And Apparatus For Protected Exchange Of Status And Secret Values Between A Video Source Application and A Video Hardware Interface

## Related Application

This application is a continuation-in-part application to U.S. Patent Applications number 09/385,590 and 09/385,592, both entitled Digital Video Content Transmission Ciphering and Deciphering Method and Apparatus, filed on August 29, 1999.

## BACKGROUND OF THE INVENTION

### 1. Field of the Invention

The present invention relates to the field of content protection. More specifically, the present invention addresses the protection accorded to exchange of status and secret values between a video source application and a video hardware interface of a video source device.

### 2. Background Information

In general, entertainment, education, art, and so forth (hereinafter collectively referred to as "content") packaged in digital form offer higher audio and video quality than their analog counterparts. However, content producers, especially those in the entertainment industry, are still reluctant in totally embracing the digital form. The primary reason being digital contents are particularly vulnerable to pirating. As unlike the analog form, where some amount of quality degradation generally occurs with each copying, a pirated copy of digital content is virtually as good as the "gold master". As a result, much effort have been spent by the industry in developing and adopting techniques to provide protection to the distribution and rendering of digital content.

Historically, the communication interface between a video source device (such as a personal computer) and a video sink device (such as a monitor) is an analog interface. Thus, very little focus has been given to providing protection for the transmission between the source and sink devices. With advances in integrated circuit and other related technologies, a new type of digital interface between video source and sink devices is emerging. The availability of this type of new digital interface presents yet another new challenge to protecting digital video content. While in general, there is a large body of cipher technology known, the operating characteristics such as the volume of the data, its streaming nature, the bit rate and so forth, as well as the location of intelligence, typically in the source device and not the sink device, present a unique set of challenges, requiring a new and novel solution. Parent applications number 09/385,590 and 09/385,592 disclosed various protocol and cipher/deciphering techniques to protect the transmission.

Similar protection challenges exist for exchanges of status and secret values between the video generating video source application and the video transmitting video hardware interface of the video source device. Thus, method and apparatus to protect these exchanges are desired.

## SUMMARY OF THE INVENTION

A video source application in a video source device requests from a video hardware interface of the video source device status with respect to a link linking the video source device to an external video sink device, and supplements the status request with a basis value to a symmetric ciphering/deciphering process. The video source application, upon receiving from the video hardware interface the requested status and a verification key, generated using a symmetric ciphering/deciphering process and employing the basis value, verifies the correctness of the verification key to determine whether to trust said provided status.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

**Figure 1** illustrates an overview of the present invention in accordance with one embodiment;

**Figures 2a-2b** illustrate a symmetric ciphering/deciphering process based method for the video hardware interface to provide sensitive information such as status and secret values to the video source application, in accordance with two embodiments;

**Figures 3a-3b** illustrate the symmetric ciphering/deciphering process of **Fig. 2a-2b** employed to facilitate provision of status and secret values from the video hardware interface to the video source application, in accordance with one embodiment each; and

**Figures 4a-4c** illustrate a one way function suitable for use to practice the symmetric ciphering/deciphering process of **Fig. 3a-3b** in further detail, in accordance with one embodiment.

## DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described, and various details will be set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention, and the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps performed in turn in a manner that is most helpful in understanding the present invention. However, the order of description should not be construed as to imply that these operations are necessarily performed in the order they are presented, or even order dependent. Lastly, repeated usage of the phrase "in one embodiment" does not necessarily refer to the same embodiment, although it may.

Referring now to **Figure 1**, wherein a block diagram illustrating an overview of the present invention, in accordance with one embodiment is shown. As illustrated, video source device **102** and video sink device **104** are coupled to each other via digital video link **106**. Video source device **102** includes video source application **108** and video hardware interface **110**. Video source application **108** generates and provides video content to video hardware interface **110**, which in turn ciphers video content and provides the video content in a ciphered form to video sink device **104** through digital video link **106** as disclosed in the aforementioned parent applications, thereby protecting video contents. Additionally, video source application **108** and video hardware interface **110** exchange various status and control information, including in particular status information about the link between video hardware interface **110** and video sink device **104**, and secret values employed by video hardware interface **110** to cipher video content as disclosed in the parent applications. In accordance with the present invention, video source application **108** and video hardware interface **110** are equipped to be able to jointly practice a symmetric ciphering/deciphering process. As a result, at least status and secret values may be provided from video hardware interface **110** to video source application **108** in a protected manner, maintaining protection to the video content being distributed to video sink device **104**.

Except for the teachings of the present invention incorporated, to be described more fully below, video source application **108** is intended to represent a broad range of video source applications known in the art, while video hardware interface **110** is substantially constituted as disclosed in the parent applications. As will be readily apparent from those skilled in the art, the present invention advantageously allows the same hardware resources of video hardware interface **110** to be used to protect the exchanges with video source application **108** as well as protecting the video content transmitted to video sink device **104**.

As disclosed in the parent applications, examples of video source device **102** includes but not limited to computers of all sizes (from palm size device to desktop device, and beyond), set-up boxes, or DVD players, whereas examples of video sink devices include but not limited to CRT monitors, flat panel displays or television sets. As to digital video link **106**, it may be implemented in any one of a number of mechanical and electrical forms, as long as they are consistent with the operating requirement (i.e. speed, bit rate and so forth), and a mechanism (which may be in hardware or through protocol) is provided to allow control information to be exchanged between video source and sink devices **102** and **104**.

Before proceeding to further described the present invention, while for ease of understanding, video source application **108** is shown to be interacting with video hardware interface **110** "directly", those skilled in the art will appreciate that typically video hardware interface **110** has an associated driver to insulate the hardware specifics from the interacting software, such as video source application **108** in this case. Accordingly, in most embodiments, video source application **108** interacts with video hardware interface **110** through its associated driver.

**Figures 2a-2b** illustrate two overviews of the symmetric ciphering/deciphering process based method for facilitating exchanges of status and control information between video source application **108** and video hardware interface **110**, in accordance with two embodiments. **Fig. 2a** is an embodiment particularly suitable for exchanges involving status and control information of short bit lengths, such as on/off status, whereas **Fig. 2b** is an embodiment particular suitable for exchanges involving status and control information of longer bit lengths, such as the secret values employed by video hardware interface **110** to cipher video contents. What constitutes short or longer bit length is application dependent. As between video hardware interface **110** and video sink device **104**, video source application **108** and video hardware interface **110** are assumed to have each been provided with an array of private "cryptographic" keys and a complementary identifier by a certification authority. In one embodiment, each of video source application **108** and video hardware interface **104** is pre-provided with an array of 40 56-bit private "cryptographic" keys by the certification authority. Cn is a 64-bit random number, and the keys are 56-bit long. For more information on the above described authentication process, see co-pending U.S. Patent Application, serial number 09/275,722, filed on March 24, 1999, entitled Method and Apparatus for the

Generation of Cryptographic Keys, having common assignee with the present application.

As illustrated in **Fig. 2a**, whenever a need occurs for video source application to retrieve a status of the short bit length type, video source application **108** first generates and provides a basis value to the symmetric ciphering/deciphering process to sink hardware interface **110**. For the illustrated embodiment, the basis value is a random number (Cn). Cn may be generated in any one of a number of techniques known in the art. Additionally, video source application **108** also provides a key selection value ($Ck_{sv}$) to video hardware interface **110**. Further, for the illustrated embodiment, which is an embodiment where the same hardware resources of video hardware interface **110** are used to satisfy video source application's request for status and control information of the short or long bit length type, video source application **108** also provides a mode indicator ($C_{mode}$) to video hardware interface **110** to denote the type of status and control information being requested. These parameters, $C_n$, $Ck_{sv}$, and $C_{mode}$ may be provided via one or more "packets", as well as in conjunction with other information.

In response, video hardware interface **110** generates an authentication key $K_u$' based on its provided array of private "cryptographic" keys Dkeys and the selection key $Ck_{sv}$ provided by video source application **108**. Video hardware interface **110** then generates the verification key $K_p$' based on the provided basis value $C_n$, the generated authentication key $K_u$', the status to be returned, and the selection key $Bk_{sv}$ it was provided by video sink device **104** for use to protectively provide video contents in a ciphered form to video sink device **104** based on a symmetric cipher/deciphering process (see parent application for further detail).

Upon generating $K_p$', for the illustrated embodiment, video hardware interface **110** returns the requested status along with $K_p$'. In one embodiment, the two values are concatenated together (S'), and returned at the same time. In alternate embodiments, it may be returned separately. Additionally, for the illustrated embodiment, video hardware interface **110** also returns $Bk_{sv}$ and $Dk_{sv}$ to video source application **108**.

Over on the video source application side, upon receipt of S', $Bk_{sv}$ and $Dk_{sv}$, video source application **108** independently generates its own copy of $K_u$ based on its array of pre-provided private "cryptographic" keys Ckeys, and $Dk_{sv}$. Next, video source application **108** independently generates its own copy of $K_p$ based on $C_n$, the returned status, and $Bk_{sv}$. Then, video source application **108** compares its independently generated $K_p$ with the received $K_p$' to determine if it should trust the status provided (when $K_p$=$K_p$') or distrust the status provided (when $K_p$=/=$K_p$').

Referring now to **Fig. 2b**, in like manner, whenever a need occurs for video source application to retrieve a control information of the longer bit length type, such as the aforementioned secret value, video source application **108** also first generates and provides a basis value to the symmetric ciphering/deciphering process to sink hardware interface **110**. Again, in one embodiment, the basis value is a random number (Cn), and it may be generated in any one of a number of techniques known in the art. Additionally, video source application **108** also provides a key selection value ($Ck_{sv}$) to video hardware interface **110**. Further, similar to the embodiment of **Fig. 2a**, where the same hardware resources of video hardware interface **110** are used to satisfy video source application's request for status and control information of the short or long bit length type, video source application **108** also provides a mode indicator ($C_{mode}$) to video hardware interface **110** to denote the type of status and control information being requested. As before, these parameters, $C_n$, $Ck_{sv}$, and $C_{mode}$ may be provided via one or more "packets", as well as in conjunction with other information.

In response, video hardware interface **110** generates an authentication key $K_u$' based on its provided array of private "cryptographic" keys Dkeys and the selection key $Ck_{sv}$ provided by video source application **108**. Video hardware interface **110** then generates a cryptographic key $K_e$' using $K_u$' and the provided basis value $C_n$.

Upon generating $K_e$', video hardware interface **110** ciphers the requested control information, e.g. secret value $M_0$', using $K_e$'. Video hardware interface **110** then returns $M_0$' in a ciphered form (M') to video source application **108**. Additionally, for the illustrated embodiment, video hardware interface **110** also returns $Dk_{sv}$ to video source application **108**.

Over on the video source application side, upon receipt of M' and $Dk_{sv}$, video source application **108** independently generates its own copy of $K_u$ based on Ckeys and $Dk_{sv}$. Next, video source application **108** independently generates its own copy of $K_e$ based on $C_n$ and $K_u$. Then, video source application **108** deciphers M', recovering $M_0$' using $K_e$.

**Figures 3a-3b** illustrate the symmetric ciphering/deciphering processes of **Fig.2a-2b** in further detail, in accordance with one embodiment each. As illustrated in **Fig. 3a**, for the exchange of status and control information of short bit length, video hardware interface **110** first generates the authentication key $K_u$' by summing its pre-provided private "cryptographic" keys Dkeys over the provided selection key $Ck_{sv}$ from video source application **108**. Upon generation of the authentication key $K_u$', video hardware interface **110** generates a first intermediate key $K_1$', ciphering the least significant 40 bits (LSB40) of the provided basis value $C_n$ by applying a one way function to it, using $K_u$'. For the illustrated embodiment, the same one way function is used for the exchange of status and control information of both short and longer bit length type. The one way function is applied in a first mode, also referred to as the A-mode, in accordance with the value of $C_{mode}$. Next, video hardware interface **110** generates a second intermediate key $K_2$' by applying the same one way function (under the same mode) to the selection key $BK_{sv}$ provided by video sink device **104**, using $K_1$'. Finally, video hardware interface **110** generates the verification key $K_p$' by applying the same one way function (under the same mode) to the status concatenated with most significant 24 bits (MSB24) of the provided basis value $C_n$, using $K_2$'.

Over on the video source application side, upon receipt of S', $Dk_{sv}$, and $BK_{sv}$, video source application **108** first independently generates its own copy of the authentication key $K_u$ by summing its selection keys Ckeys over $Dk_{sv}$. Upon generation of the authentication key $K_u$, video source application **108** independently generates its own copy of the first intermediate key $K_1$ by applying a similar one way function to the least significant 40 bits (LSB40) of the basis value $C_n$ provided to video hardware interface **110**, using $K_u$. Video source application **108** also uses the same one way function to facilitate the exchange of status and control information of both short and longer bit length type. Thus, the common one way function is applied in the earlier described first mode, also referred to as the A-mode, in accordance with the value of $C_{mode}$. Next, video source application **108** independently generates its own copy of the second intermediate key $K_2$ by applying the same one way function (under the same mode) to the selection key $BK_{sv}$, using $K_1$. Finally, video source application **108** independently generates its own copy of $K_p$ by applying the same one way function (under the same mode) to the status concatenated with the most significant 24 bits (MSB24) of the basis value $C_n$, using $K_2$.

**Fig. 3b** illustrates the embodiment for handling the exchange of status and control information of longer bit length, video hardware interface **110** first generates the authentication key $K_u$' by summing its selected one of the pre-provided private "cryptographic" keys over the provided selection key from video source application **108**. Upon generation of the authentication key $K_u$', video hardware interface **110** generates another intermediate key $K_4$' by applying a one way function to the least significant 40 bits (LSB40) of the provided basis value $C_n$, using $K_u$'. For the illustrated embodiment, the same one way function is used for the exchange of status and control information of both short and longer bit length type. The one way function is applied in a second mode, also referred to as the B-mode, in accordance with the value of $C_{mode}$. Next, video hardware interface **110** generates $K_e$', the ciphering key, by applying the same one way function (under the same mode) to the most significant 24 bits (MSB24) of the provided basis value $C_n$, using $K_4$'.

Over on the video source application side, upon receipt of M' and $Dk_{sv}$, video source application **108** first independently generates its own copy of the authentication key $K_u$ by summing its array of private "cryptographic" keys Ckeys over $Dk_{sv}$. Upon generation of the authentication key $K_u$, video source application **108** independently generates its own copy of intermediate key $K_4$ by applying a similar one way function to the least significant 40 bits (LSB40) of the basis value $C_n$, using $K_u$. Video source application **108** also uses the same one way function to facilitate the exchange of status and control information of both short and longer bit length type. Thus, the common one way function is applied in the earlier described second mode, also referred to as the B-mode, in accordance with the value of $C_{mode}$. Next, video source application **108** independently generates its own copy of $K_p$, the deciphering key, by applying the same one way function (under the same mode) to the most significant 24 bits (MSB24) of the basis value $C_n$, using $K_1$.

In one embodiment, $K_1$ and $K_4$ are generated only by video source application **108**, once per "session", using highly protected Ckeys, and stored in the application for later use for the remainder of the session. In other words, compromise of K1 or K4 allows "attack" for only one session (compromise of Ckeys would allow "attack" for unlimited number of sessions). This approach has the following advantages. Since $Dk_{sv}$ is a constant, video source application **108** can fix the least significant 40 bits of $C_n$, and change only the most significant 24 bits of $C_n$ for different status and information requests, thereby allowing video source application **108** to rerun the protocol for different requests at the computation of $K_1$ and $K_4$ and speed up the transfer of these information.

**Figures 4a-4c** illustrate a one-way function suitable for use to practice the symmetric ciphering/deciphering process of **Fig. 3a-3b**, in accordance with one embodiment. As illustrated in **Fig. 4a**, the one way function **800** includes a number of linear feedback shift registers (LFSRs) **802** and combiner function **804**, coupled to each other as shown. LFSRs **802** and combiner function **804** are collectively initialized with the appropriate keys and data values, depending the mode of operation $C_{mode}$. During operation, the values are successively shifted through LFSRs **802**. Selective outputs are taken from LFSRs **802**, and combiner function **804** is used to combine the selective outputs to generate the desired outputs.

In one embodiment, four LFSRs of different lengths are employed. Three sets of outputs are taken from the four LFSRs. The polynomials represented by the LFSR and the bit positions of the three sets of LFSR outputs are given by the table to follow:

| LFSR | Polynomial | Combining Function Taps | | |
|---|---|---|---|---|
| | | 0 | 1 | 2 |
| 3 | $x^{27} + x^{24} + x^{21} + x^{17} + x^{13} + x^{8} + 1$ | 8 | 17 | 26 |
| 2 | $x^{26} + x^{23} + x^{18} + x^{15} + x^{12} + x^{8} + 1$ | 8 | 16 | 25 |
| 1 | $x^{24} + x^{21} + x^{18} + x^{14} + x^{10} + x^{7} + 1$ | 7 | 15 | 23 |
| 0 | $x^{23} + x^{20} + x^{16} + x^{12} + x^{9} + x^{6} + 1$ | 7 | 14 | 22 |

The initialization of the LFSRs and the combiner function, more specifically, the shuffling network of the combiner function, is in accordance with the following table.

| | Bit Field | One Way-A Initial Value | One Way-B Initial Value |
|---|---|---|---|
| LFSR3 | [26:22] | Data [39:35] | Data[34:30] |
| | [21] | inverse of LFSR3 initialization bit [9] | inverse of LFSR3 initialization bit [9] |
| | [20:14] | Data[34:28] | Data[29:23] |
| | [13:0] | Key[55:42] | Key[48:35] |
| LFSR2 | [25:22] | Data[27:24] | Data[22:19] |
| | [21] | inverse of LFSR2 initialization bit [8] | inverse of LFSR2 initialization bit [8] |
| | [20:14] | Data[23:17] | data[18:12] |
| | [13:0] | Key[41:28] | Key[34:21] |
| LFSR1 | [23:19] | Data[16:12] | Data[11:7] |

| | | | |
|---|---|---|---|
| | [18] | inverse of LFSR1 initialization bit [5] | inverse of LFSR1 initialization bit [5] |
| | [17:14] | Data[11:8] | Data[6:3] |
| | [13:0] | Key[27:14] | Key[20:7] |
| LFSR0 | [22:20] | Data[7:5] | Data[2:0] |
| | [19] | inverse of LFSR0 initialization bit [10] | inverse of LFSR0 initialization bit [10] |
| | [18:14] | Data[4:0] | Data[39:35] |
| | [13:7] | Key[13:7] | Key[6:0] |
| | [6:0] | Key[6:0] | Key[55:49] |
| Shuffle | Register A | 0 | 0 |
| Network | Register B | 1 | 1 |

Data are LSB40($C_n$), $BK_{sv}$ and MSB24($C_n$), whereas Keys are $K_u$, $K_1$, $K_2$ and $K_4$.

The combined result is generated from the third set of LFSR outputs, using the first and second set of LFSR outputs as data and control inputs respectively to combiner function **804**. The third set of LFSR outputs are combined into a single bit.

**Fig. 4b** illustrates combiner function **804** in further detail, in accordance with one embodiment. As illustrated, combiner function **804** includes shuffle network **806** and XOR **808a-808b**, serially coupled to each other and LFSRs **802** as shown. For the illustrated embodiment, shuffle network **806** includes four binary shuffle units **810a-810d** serially coupled to each other, with first and last binary shuffle units **810a** and **810d** coupled to XOR **808a** and **808b** respectively. XOR **808a** takes the first group of LFSR outputs and combined them as a single bit input for shuffle network **806**. Binary shuffle units **810a-810d** serially propagate and shuffle the output of XOR **808a**. The second group of LFSR outputs are used to control the shuffling at corresponding ones of binary shuffle units **810a-810d**. XOR **808b** combines the third set of LFSR outputs with the output of last binary shuffle unit **810d**.

**Fig. 4c** illustrates one binary shuffle unit **810*** (where * is one of **a-d**) in further detail, in accordance with one embodiment. Each binary shuffle unit **810*** includes two flip-flops **812a** and **812b**, and a number of selectors **814a-814c**, coupled to each other as shown. Flip-flops **812a** and **812b** are used to store two state values (A, B). Each selector **814a**, **814b** or **814c** receives a corresponding one of the second group of LFSR outputs as its control signal. Selector **814a-814b** also each receives the output of XOR **808a** or an immediately preceding binary shuffle unit **810*** as input. Selector **814a-814b** are coupled to flip-flops **812a-812b** to output one of the two stored state values and to shuffle as well as modify the stored values in accordance with the state of the select signal. More specifically, for the illustrated embodiment, if the stored state values are (A, B), and the input and select values are (D, S), binary shuffle unit **810*** outputs A, and stores (B, D) if the value of S is "0". Binary shuffle unit **810*** outputs B, and stores (D, A) if the value of S is "1".

In one embodiment, once the data values are loaded into the registers and the shuffle networks, the one-way function is clocked for 32 clocks to mix the data and key bits. During this warm up period, the 32 output bits are discarded. As a result, the initial output stream is a non-linear function of many key and data bits. In alternate embodiments, depending on the desired robustness level, the present invention may be practiced with shorter or longer warm up period.

Those skilled in the art will appreciate that this one way function substantially parallel one embodiment of the one way function disclosed in the parent applications for the cipher employed by video hardware interface **110** to cipher video content to be transmitted to video sink device **104**. Accordingly, video hardware interface **110** may employ the same one way function to facilitate exchange of status and control information with video source application **108** in a protected manner, as well as to cipher video content for video sink device **104**.

Accordingly, a novel method and apparatus for ciphering and deciphering video content to protect the video content from unauthorized copying during transmission has been described.

Epilogue

From the foregoing description, those skilled in the art will recognize that many other variations of the present invention are possible. Thus, the present invention is not limited by the details described, instead, the present invention can be practiced with modifications and alterations within the spirit and scope of the appended claims.

CLAIMS

What is claimed is:

1. In a video source device, a method comprising:

a video source application requesting from a video hardware interface status with respect to a link linking said video source device to an external video sink device, and supplementing said status request with a first basis value to a symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested status and a verification key, generated through said symmetric ciphering/deciphering process employing said first basis value; and

the video source application verifying the correctness of said verification key to determine whether to trust said provided status.

2. The method of claim 1, wherein said method further comprises said video source application supplementing said status request with a selection key for the video hardware interface to use to generate an authentication key for use to generate said verification key.

3. The method of claim 1, wherein said verification of the correctness of the received verification key comprises said video source application independently generating its own copy of the verification key.

4. The method of claim 3, wherein said independent generation of said video source application's own copy of said verification key comprises said video source

application independently generating its own copy of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

5. The method of claim 3, wherein said independent generation of said video source application's own copy of said verification key comprises said video source application applying a one way function to at least a first selected subset of said first basis value provided to said video hardware interface using an independently generated copy of an authentication key.

6. The method of claim 5, wherein said independent generation of said video source application's own copy of said verification key further comprises said video source application applying said one way function to a selection key said video hardware interface received from said video sink device for use by said video hardware interface to authenticate said video sink device, using the result of said first application of the one-way function.

7. The method of claim 6, wherein said independent generation of said video source application's own copy of said verification key further comprises said video source application applying said one way function to at least a second selected subset of said first basis value provided to said video hardware interface using the result of said second application of the one-way function.

8. The method of claim 6, wherein said independent generation of said video source application's own copy of said verification key further comprises said video

source application applying said one way function to at least said status using the result of said second application of the one-way function.

9. The method of claim 1, wherein said method further comprises

said video source application requesting from said video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, and supplementing said secret request with a second basis value to said symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered with a ciphering key generated using said symmetric ciphering/deciphering process and employing said second basis value; and

the video source application deciphering said ciphered secret using an independently generated copy of said ciphering key.

10. The method of claim 9, wherein said method further comprises said video source application supplementing said secret request with a selection key for the video hardware interface to use to generate an authentication key for use by said symmetric ciphering/deciphering process.

11. The method of claim 9, wherein said method further comprises said video source application independently generating its own copy of the ciphering key.

12. The method of claim 11, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source

application independently generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

13. The method of claim 11, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application applying a one way function to at least a first selected subset of said second basis value provided to said video hardware interface using an independently generated copy of an authentication key.

14. The method of claim 13, wherein said independent generation of said video source application's own copy of said ciphering key further comprises said video source application applying said one way function to at least a second selected subset of said second basis value provided to said video hardware interface using the result of said first application of the one-way function.

15. In a video source device, a method comprising:

a video source application requesting from a video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, and supplementing said secret request with a basis value to said symmetric ciphering/deciphering process;

the video source application receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value; and the video source application deciphering said ciphered secret using an independently generated copy of said ciphering key.

16. The method of claim 15, wherein said method further comprises said video source application supplementing said secret request with a selection key for the video hardware interface to use to generate an authentication key for use by said symmetric ciphering/deciphering process.

17. The method of claim 15, wherein said method further comprises said video source application independently generating its own copy of the ciphering key.

18. The method of claim 17, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application independently generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

19. The method of claim 17, wherein said independent generation of said video source application's own copy of said ciphering key comprises said video source application applying a one way function to at least a first selected subset of said basis value provided to said video hardware interface using an independently generated copy of an authentication key.

20. The method of claim 19, wherein said independent generation of said video source application's own copy of said ciphering key further comprises said video source application applying said one way function to at least a second selected

subset of said basis value provided to said video hardware interface using the result of said first application of the one-way function.

21. In a video source device, a method comprising:

a video hardware interface receiving from a video source application a request for status with respect to a link linking said video source device to an external video sink device, and said status request being supplemented with a first basis value to a symmetric ciphering/deciphering process;

the video hardware interface returning said requested status to said video source application, and accompanying said returned requested status with a verification key, generated using said symmetric ciphering/deciphering process and employing said first basis value, to allow said video source application to determine whether to trust said returned status.

22. The method of claim 21, wherein said method further comprises said video hardware interface further accompanying said returned status with a selection key for the video source application to use to independently generate its own copy of an authentication key for use to independently generate its own copy of said verification key.

23. The method of claim 21, wherein said generation of said verification key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

24. The method of claim 21, wherein said generation of said verification key comprises said video hardware interface applying a one way function to at least a first selected subset of said first basis value using an authentication key.

25. The method of claim 24, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to a selection key said video hardware interface received from said video sink device for use by said video hardware interface to authenticate said video sink device, using the result of said first application of the one-way function.

26. The method of claim 25, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to at least a second selected subset of said first basis value using the result of said second application of the one-way function.

27. The method of claim 25, wherein said generation of said verification key further comprises said video hardware interface applying said one way function to at least said status using the result of said second application of the one-way function.

28. The method of claim 21, wherein said method further comprises

said video hardware interface receiving from said video source application request for a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, said secret request being also supplemented with a second basis value to said symmetric ciphering/deciphering process; and said video hardware interface returning said requested secret in a ciphered form to said video source application, the secret having been ciphered by a ciphering key generated using said symmetric ciphering/deciphering process and employing said second basis value.

29. The method of claim 28, wherein said method further comprises said video hardware interface receiving from said video source application a selection key supplementing said secret request for the video hardware interface to use to generate an authentication key for use in said symmetric ciphering/deciphering process.

30. The method of claim 28, wherein said generation of said ciphering key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

31. The method of claim 28, wherein said generation of said ciphering key comprises said video hardware interface applying a one way function to at least a first selected subset of said second basis value using an authentication key.

32. The method of claim 31, wherein said generation of said ciphering key further comprises said video hardware interface applying said one way function to at least a second selected subset of said second basis value using the result of said first application of the one-way function.

33. In a video source device, a method comprising

a video hardware interface receiving from a video source application request for a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, said secret request being supplemented with a basis value to a symmetric ciphering/deciphering process; and

said video hardware interface returning said requested secret in a ciphered form to said video source application, the secret having been ciphered by a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value.

34. The method of claim 33, wherein said method further comprises said video hardware interface receiving from said video source application a selection key supplementing said secret request for the video hardware interface to use to generate an authentication key for use in said symmetric ciphering/deciphering process.

35. The method of claim 33, wherein said generation of said ciphering key comprises said video hardware interface generating an authentication key by summing a plurality of cryptographic keys over a selection key received from said video source application.

36. The method of claim 33, wherein said generation of said ciphering key comprises said video hardware interface applying a one way function to at least a first selected subset of said basis value using an authentication key.

37. The method of claim 36, wherein said generation of said ciphering key further comprises said video hardware interface applying said one way function to at least a second selected subset of said basis value using the result of said first application of the one-way function.

38. An article of manufacture comprising:

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from a video hardware interface status with respect to a link linking said video source device to an external video sink device, and supplements said status request with a basis value to a symmetric ciphering/deciphering process, when the programming instructions are executed by a processor, the video source application, upon receiving from said video hardware interface said requested status and a verification key generated using said symmetric ciphering/deciphering process and employing said basis value, further verifies the correctness of said verification key to determine whether to trust said provided status.

39. The article of manufacture of claim 38, wherein as part of said verification of the correctness of the received verification key, said video source application independently generates its own copy of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

40. The article of manufacture of claim 38, wherein as part of said verification of the correctness of the received verification key, said video source application applies a one way function to at least a first selected subset of said basis value

provided to said video hardware interface using an independently generated copy of an authentication key.

41. An article of manufacture comprising:

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from a video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to an external video sink device, and supplements said secret request with a basis value to said symmetric ciphering/deciphering process, when the programming instructions are executed by a processor, the video source application, upon receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value, further deciphers said ciphered secret using an independently generated copy of said ciphering key.

42. The article of manufacture of claim 41, wherein said video source application independently generates its own copy of said ciphering key, including generation of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

43. The article of manufacture of claim 41, wherein said video source application independently generates its own copy of said ciphering key, including application of a one way function to at least a first selected subset of said basis value provided to said video hardware interface, using an independently generated copy of an authentication key.

44. An apparatus comprising:

a video hardware interface equipped to securely transmit digital video to an external video sink device coupled to said apparatus by way of said video hardware interface;

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from said video hardware interface status with respect to said coupling between said video hardware interface and said external video sink device, and supplements said status request with a basis value to a symmetric ciphering/deciphering process, when the programming instructions are executed, the video source application, upon receiving from said video hardware interface said requested status and a verification key, generated using said symmetric ciphering/deciphering process and employing said basis value, further verifies the correctness of said verification key to determine whether to trust said provided status; and

a processor coupled to said storage medium and said video hardware interface to execute said programming instructions.

45. The apparatus of claim 44, wherein said video source application independently generates its own copy of the verification key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface, for use to verify the correctness of the received verification key.

46. The apparatus of claim 44, wherein as part of said verification of the correctness of the received verification key, said video source application applies a one way function to at least a first selected subset of said basis value provided to

said video hardware interface using an independently generated copy of an authentication key.

47. An apparatus comprising:

a video hardware interface equipped to securely transmit digital video to an external video sink device coupled to said apparatus by way of said video hardware interface;

a storage medium having stored therein a plurality of programming instructions implementing a video source application that requests from said video hardware interface a secret employed by said video hardware interface to cipher video to be transmitted by said video hardware interface to said external video sink device, and supplements said secret request with a basis value to said symmetric ciphering/deciphering process, when the programming instructions are executed, the video source application, upon receiving from said video hardware interface said requested secret in a ciphered form, having been ciphered using a ciphering key generated using said symmetric ciphering/deciphering process and employing said basis value, further deciphers said ciphered secret using an independently generated copy of said ciphering key; and

a processor coupled to said storage medium and said video hardware interface to execute said programming instructions.

48. The apparatus of claim 47, wherein said video source application independently generates its own copy of said ciphering key, including generation of an authentication key by summing a plurality of cryptographic keys over a selection key received from said video hardware interface.

49. The apparatus of claim 47, wherein said video source application independently generates its own copy of said ciphering key, including application of a one way function to at least a first selected subset of said basis value provided to said video hardware interface using an independently generated copy of an authentication key.

## ABSTRACT OF THE DISCLOSURE

A video source application in a video source device requests from a video hardware interface of the video source device status with respect to a link linking the video source device to an external video sink device, and supplements the status request with a first basis value to a symmetric ciphering/deciphering process. The video source application, upon receiving from the video hardware interface the requested status and a verification key, generated using said symmetric ciphering/deciphering process and employing the first basis value, verifies the correctness of the verification key to determine whether to trust said provided status. In like manner, the video source application requests from the video hardware interface a secret the video hardware interface uses to cipher video to be transmitted by the video hardware interface to the external video sink device. The secret request is supplemented with a second basis value to the symmetric ciphering/deciphering process. The secret is returned in a cipher form, ciphered using a ciphering key generated using the second basis value. The video source application deciphers the secret using its own independently generated copy of the ciphering key.

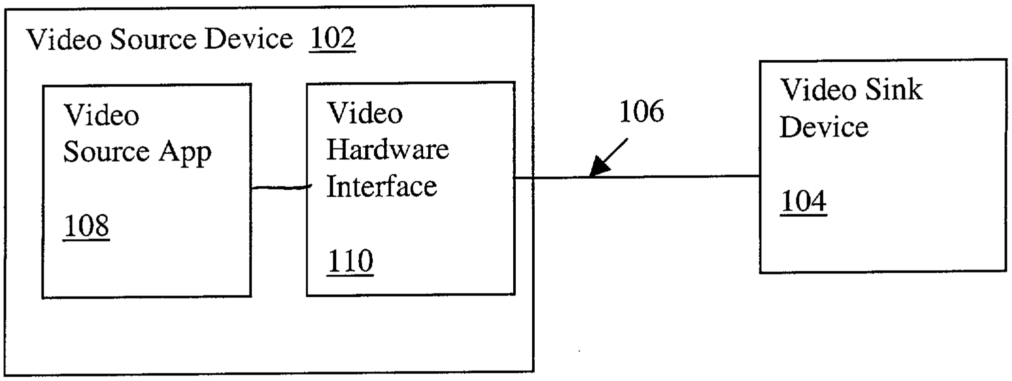
Video Source Device 102
Video Source App
108
Video Hardware Interface
110
106
Video Sink Device
104

Figure 1

| Video Source Application | | Video Hardware Interface |
|---|---|---|
| Generate $C_n$ | $C_n$, $Ck_{sv}$, $C_{mode}$<br>→ | Generate $K_u$' ($Ck_{sv}$, $Dk_{sv}$)<br>Generate $K_p$' ($K_u$', $C_n$, $Bk_{sv}$) |
| Generate $K_u$ ($Ck_{sv}$, $Dk_{sv}$)<br>Generate $K_p$ ($K_u$, $C_n$, $Bk_{sv}$) | S', $Bk_{sv}$, $Dk_{sv}$<br>← | Generate S' = status \|\| $K_p$' |
| Determine if $K_p$=$K_p$' | | |

**Figure 2a**

| Video Source Application | | Video Hardware Interface |
|---|---|---|
| Generate $C_n$ | $C_n$, $Ck_{sv}$, $C_{mode}$<br>→ | Generate $K_u$' ($Ck_{sv}$, $Dk_{sv}$)<br>Generate $K_e$' ($K_u$', $C_n$) |
| Generate $K_u$ ($Ck_{sv}$, $Dk_{sv}$)<br>Generate $K_e$ ($K_u$, $C_n$) | M', $Dk_{sv}$<br>← | M' = $K_e$' XOR $M_0$' |
| $M_0$' = $K_e$ XOR M' | | |

**Figure 2b**

| Video Source Application | | Video Hardware Interface |
|---|---|---|
| | | $K_u$' = ∑ Dkeys over $Ck_{sv}$<br>$K_1$' = OneWay-A ($K_u$', LSB40($C_n$))<br>$K_2$' = OneWay-A ($K_1$', $Bk_{sv}$)<br>$K_p$' = OneWay-A ($K_2$', status‖MSB24($C_n$)) |
| $K_u$ = ∑ Ckeys over $Dk_{sv}$<br>$K_1$ = OneWay-A ($K_u$, LSB40($C_n$))<br>$K_2$ = OneWay-A ($K_1$, $Bk_{sv}$)<br>$K_p$ = OneWay-A ($K_2$, status‖MSB24($C_n$)) | | |

**Figure 3a**

| Video Source Application | | Video Hardware Interface |
|---|---|---|
| | | $K_u$' = ∑ Dkeys over $Ck_{sv}$<br>$K_4$' = OneWay-B ($K_u$', LSB40($C_n$))<br>$K_e$' = OneWay-B ($K_4$', MSB24($C_n$)) |
| $K_u$ = ∑ Ckeys over $Dk_{sv}$<br>$K_4$ = OneWay-B ($K_u$, LSB40($C_n$))<br>$K_e$ = OneWay-B ($K_4$, MSB24($C_n$)) | | |

**Figure 3b**

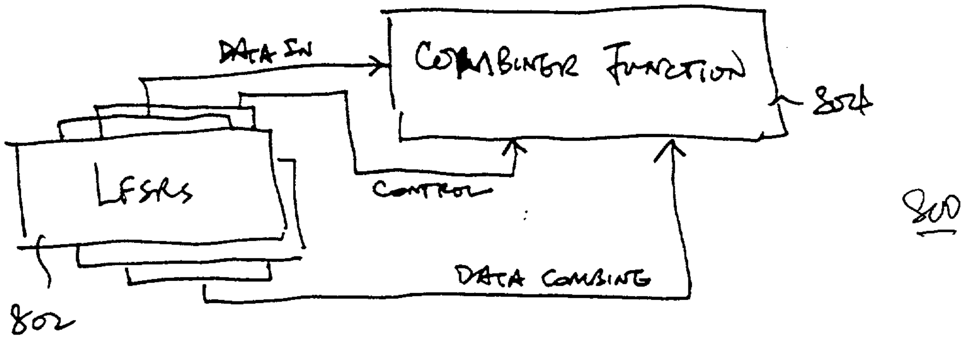

FIG. 4a

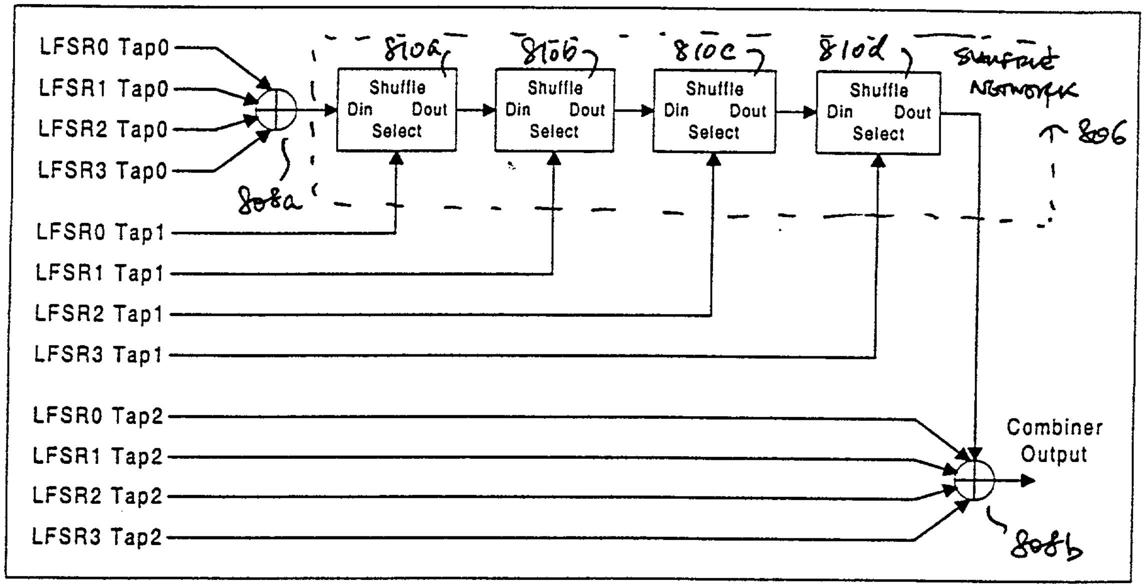

FIG. 4b

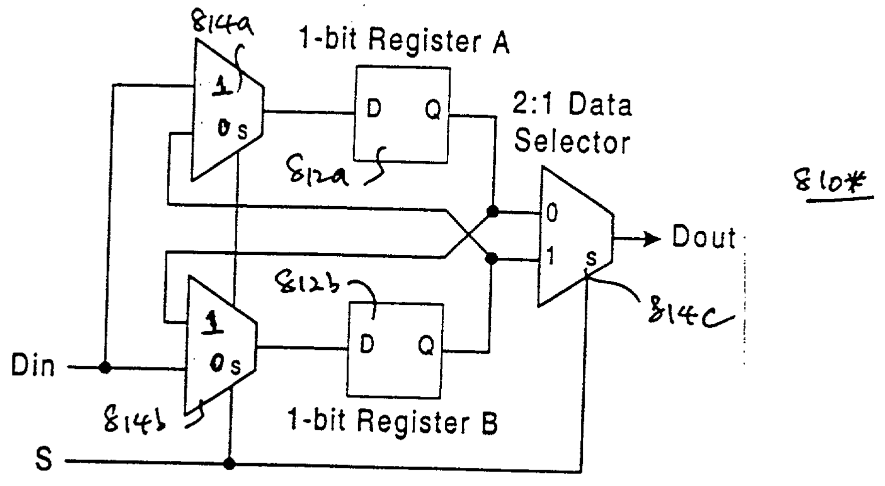

FIG. 4c

Attorney's Docket No.: 42390.P7948 PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**METHOD AND APPARATUS FOR PROTECTED EXCHANGE OF STATUS AND SECRET VALUES BETWEEN A VIDEO SOURCE APPLICATION AND A VIDEO HARDWARE INTERFACE**

the specification of which

XX is attached hereto.
____ was filed on ______________________ as
United States Application Number ______________
or PCT International Application Number ______________
and was amended on ______________________.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

| Prior Foreign Application(s) | | | Priority Claimed | |
|---|---|---|---|---|
| (Number) | (Country) | (Day/Month/Year Filed) | Yes | No |
| (Number) | (Country) | (Day/Month/Year Filed) | Yes | No |
| (Number) | (Country) | (Day/Month/Year Filed) | Yes | No |

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

(Application Number) Filing Date

(Application Number) Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

| | | |
|---|---|---|
| 09/385,590 | 8/29/99 | Pending |
| (Application Number) | Filing Date | (Status -- patented, pending, abandoned) |
| 09/385,592 | 8/29/99 | Pending |
| (Application Number) | Filing Date | (Status -- patented, pending, abandoned) |

I hereby appoint William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. P44,587; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Erica W. Kuo, Reg. No. 42,775; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. P44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Kimberley G. Nobles, Reg. No. 38,255; Daniel E. Ovanezian, Reg. No. 41,236; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. P45,241; Steven D. Yates, Reg. No. 42,242; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; Paramita Ghosh, Reg. No. 42,806; and Sang Hui Kim, Reg. No. 40,450; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. P44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Aloysius T.C. AuYeung , BLAKELY, SOKOLOFF, TAYLOR
(Name of Attorney or Agent)
& ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025
and direct telephone calls to Aloysius T.C. AuYeung , (503) 684-6200.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Robert W. Faber

Inventor's Signature ______________________ Date ______________

Residence Hillsboro, Oregon Citizenship USA
(City, State) (Country)

Post Office Address 942 NE Third Avenue
Hillsboro, Oregon 97124

Full Name of Second/Joint Inventor David A. Lee

Inventor's Signature ______________________ Date ______________

Residence Beaverton, Oregon Citizenship USA
(City, State) (Country)

Post Office Address 740 SW Willow Creek Drive
Beaverton, Oregon 97006

Full Name of Third/Joint Inventor Brendan S. Traw

Inventor's Signature ______________________ Date ______________

Residence Portland, Oregon Citizenship USA
(City, State) (Country)

Post Office Address 10859 NW Supreme Court
Portland, Oregon 97229

Full Name of Fourth/Joint Inventor Gary L. Graunke

Inventor's Signature ______________________ Date ______________

Residence Hillsboro, Oregon Citizenship USA
(City, State) (Country)

Post Office Address 362 NE Hillwood Drive
Hillsboro, Oregon 97124

Full Name of Fifth/Joint Inventor Richard P. Mangold

Inventor's Signature ______________ Date ______________

Residence Forest Grove, Oregon Citizenship USA
(City, State) (Country)

Post Office Address 7155 NW Kansas City Road
Forest Grove, Oregon 97116

Full Name of Sixth/Joint Inventor ______________

Inventor's Signature ______________ Date ______________

Residence ______________ Citizenship ______________
(City, State) (Country)

Post Office Address ______________

Full Name of Seventh/Joint Inventor ______________

Inventor's Signature ______________ Date ______________

Residence ______________ Citizenship ______________
(City, State) (Country)

Post Office Address ______________

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.